CONSIDERATIONS FOR FINANCIAL INSTITUTIONS TO PREVENT AND DETECT ACCOUNT TAKEOVER FRAUD

Effective account takeover fraud prevention and detection can make it harder for criminals to succeed in committing payments fraud. By combining proactive intelligence and behavioral monitoring, financial institutions can strengthen their layered shields against evolving account takeover fraud threats.

GATHERING INTELLIGENCE TO STAY AHEAD OF ACCOUNT TAKEOVER FRAUD

As introduced in Module 2, the beginning of the account takeover fraud lifecycle is the harvesting phase, when criminals seek account credentials and other personal information to impersonate the account holder. With the help of industry partners, financial institutions can track these early-stage activities that may signal heightened account takeover fraud risks.

For example, usernames and passwords may be published on the dark web after a large-scale data breach, allowing criminals to use them for fraud. By partnering with vendors or industry consortiums that provide compromised credential lists, financial institutions can flag accounts that may be at higher risk and take steps to reduce that risk, including requiring password resets or adding extra authentication steps. Similarly, financial institutions can monitor direct attacks against their institutions, such as organized phishing campaigns (e.g., sending texts or emails to financial institution employees) or a sudden surge in login attempts, which can indicate mass credential-stuffing attempts.

By combining external threat feeds with internal behavioral insights, financial institutions can build a stronger foundation for preventing and detecting account takeover fraud attempts before they impact customers.

DETECTING AND VALIDATING LEGITIMATE ENTRY POINTS

A critical step in preventing account takeover fraud is ensuring that every attempt to access an account comes from the authorized user. Financial institutions may want to look beyond simple username and password checks and adopt a layered approach that combines Multi-Factor Authentication (MFA), device intelligence and behavioral signals. MFA plays a central role in this strategy because it requires customers to verify their identities through more than one method, making it harder for attackers to use stolen or guessed credentials. It also can help financial institutions distinguish between routine user activity and suspicious access attempts, especially when login behavior, device characteristics or location patterns do not align with a customer's typical activity. By tying user verification to an additional factor that criminals cannot easily replicate, MFA becomes essential to detect anomalies and stop fraudulent logins before they result in account takeover fraud.

CONSIDERATIONS FOR FINANCIAL INSTITUTIONS TO PREVENT AND DETECT ACCOUNT TAKEOVER FRAUD

For example, evaluating a blend of device and identity signals could improve fraud detection capabilities. When a customer logs in, consider these questions:

- Is this the customer's usual device?
- Does the IP address match their typical location?
- Has the user recently changed the phone number or email address associated with the account?

Such checks rely on near-real-time data and pattern analysis that usually does not impact the customer experience. Sudden changes in behavior or devices, such as a login from an unfamiliar device in a new country, can prompt additional verification steps. If anomalous signals are identified, the financial institution may seek to work with third-party data providers for more insights. For example, a mobile data provider could determine if there was a recent change in the account holder's SIM card, which could indicate that the associated mobile device has been compromised.

STOP ACCOUNT TAKEOVER FRAUD BEFORE IT ESCALATES: MONITORING ACCOUNT AND TRANSACTION ACTIVITY

Once criminals gain access to an account, their next step is monetization: moving funds out of the account. For financial institutions, this stage is also critical because it often provides the clearest signals of account takeover fraud in progress. Detecting and responding quickly can help prevent losses and build customer trust.

For example, transaction monitoring can identify unusual patterns, sudden large transfers, multiple payments to new recipients, or rapid withdrawals. These behaviors often stand out when compared to a customer's normal activity. Even straightforward rules, such as flagging transactions above a certain threshold or outside typical geographic regions, can help identify high-risk events.

CONSIDERATIONS FOR FINANCIAL INSTITUTIONS TO PREVENT AND DETECT ACCOUNT TAKEOVER FRAUD

TRANSACTION MONITORING IN ACTION

STEP 1: Transaction Monitoring Begins

- The financial institution's fraud detection system continuously monitors Jane's account activity using transaction monitoring rules and behavioral analytics.

STEP 2: Unusual Pattern Detected

- Jane initiates a $15,000 wire transfer to a new recipient in Eastern Europe. This is 15 times higher than her usual transfer amount and to a region with which she has never interacted before.
- **System Action: Rules Triggered**
  - » Threshold rule: Flag transactions above $10,000.
  - » Geographic rule: Flag transactions outside typical regions (USA → Eastern Europe).
  - » Risk score increases significantly.

STEP 3: Additional Suspicious Behavior

- Within 30 minutes, Jane makes three more transfers of $5,000 each to different new payees.
- Total outflow in one hour: $30,000 (normal monthly outflow: $1,000).
- Fraud detection engine assigns high-risk status to the account.

STEP 4: Automated Response & Possible Actions:

- Hold transactions temporarily.
- Send alert to fraud operations team.
- Contact customer to investigate.

It is equally important to monitor account changes. To facilitate account takeover fraud, criminals frequently update contact details to intercept alerts or reset one-time passcodes and account passwords. Financial institutions should consider these to be high-risk events. When they occur, financial institutions can consider implementing step-up authentication to ensure the request is legitimate.

Finally, alerting customers about high-volume or high-value transactions, as well as account profile changes, gives them a chance to quickly confirm or dispute activity. This proactive protection may help stop fraud and reinforce trust in the financial institution. By combining transaction monitoring, risk-based authentication and timely customer engagement, financial institutions can disrupt monetization attempts and protect both their clients and their reputations.

CONSIDERATIONS FOR FINANCIAL INSTITUTIONS TO PREVENT AND DETECT ACCOUNT TAKEOVER FRAUD

CONCLUSION: BUILDING A STRONGER SHIELD AGAINST ACCOUNT TAKEOVER FRAUD

Account takeover fraud attacks pose significant threats to financial institutions and their customers. For financial institutions, the key to prevention and detection lies in a proactive, layered approach that combines both intelligence and monitoring,

By utilizing threat intelligence, financial institutions potentially can identify risks of account takeover fraud attacks and emerging fraud patterns before criminals can strike. Pairing this with access validation, as well as checking device signals, IP addresses and behavioral consistency, helps ensure that only legitimate users enter the system. Monitoring monetization attempts through transaction analysis and high-risk event alerts provides a critical safety net when criminals try to move funds or change account details.

At the same time, account takeover fraud prevention and detection is an ongoing effort. As fraud tactics evolve, so must financial institutions' prevention and detection strategies. By staying vigilant and investing in these foundational practices, financial institutions can build a stronger shield to reduce losses and protect their customers from ongoing threats.

TAKE THE NEXT STEP:
PREVENTING ACCOUNT TAKEOVER FRAUD FOR FINANCIAL SERVICES ORGANIZATIONS

Harvest Threat Intelligence: Monitor for leaked credentials and external attack indicators. Use industry feeds and consortium data to identify compromised accounts early.

Validate Access Signals: Go beyond passwords. Check device consistency, IP addresses and linked contact details to confirm legitimate account access.

Monitor for Monetization Attempts: Watch for unusual transactions or account changes, such as large transfers or changes in contact information, which may signal fraud in progress.

Use Step-Up Authentication and Alerts: When high-risk events occur, apply additional verification steps and promptly notify customers to confirm their legitimacy.

Adopt a Layered Approach: Combine intelligence, behavioral monitoring and customer engagement to create a strong, proactive defense against evolving account takeover fraud threats.

The account takeover fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about scams and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.